

## Edycja uprawnień - karta

Określa, jak Internet Explorer ma obsługiwać ca<sup>31</sup> zawartość oraz uprawnienia wymagane przez podpisane i nie podpisane aplety Java.

Ustawienia dla uprawnień nie podpisanych i podpisanych wp<sup>31</sup>ywa<sup>1</sup> na:

[Chroniona przestrzeń dostępna](#)

[Dialogi](#)

[Dostęp do plików wybrany przez użytkownika](#)

[Dostęp do wszystkich adresów sieciowych](#)

[Dostęp do wszystkich plików](#)

[Drukowanie](#)

[Informacje o systemie](#)

[Wykonywanie](#)

### Uruchamiaj niepodpisane zawartość

Uprawnienia możesz określić indywidualnie, ustawiając w polu **Uruchamiaj niepodpisane zawartość** wartość **Uruchamiaj w piaskownicy**. Następnie możesz zresetować oddzielnie każde uprawnienie, nadając mu wartość **Wy<sup>31</sup>cz** lub **W<sup>31</sup>cz** w polu **Uruchamiaj niepodpisane zawartość**. Jeżeli wybierzesz wartość **Wy<sup>31</sup>cz** lub **W<sup>31</sup>cz** w polu **Uruchamiaj niepodpisane zawartość**, ustawienie to będzie stosowane dla wszystkich uprawnień w obszarze **Dodatkowe niepodpisane uprawnienia**.

Wybierz jedną z następujących możliwości dla pola **Uruchamiaj niepodpisane zawartość**:

- Aby uruchomić nie podpisane zawartość jedynie z uprawnieniami dozwolonymi w „piaskownicy”, kliknij opcję **Uruchamiaj w piaskownicy**. Jeżeli wybierzesz tę opcję, możesz zresetować oddzielnie każde uprawnienie, nadając mu wartość **Wy<sup>31</sup>cz** lub **W<sup>31</sup>cz**.
- Aby automatycznie odrzucać nie podpisane zawartość bez monitorowania, kliknij opcję **Wy<sup>31</sup>cz**. Wszystkie uprawnienia w polu **Dodatkowe niepodpisane uprawnienia** mają przypisaną wartość **Wy<sup>31</sup>cz**; nie można indywidualnie zresetować żadnego uprawnienia do wartości **W<sup>31</sup>cz**.
- Aby automatycznie akceptować nie podpisane zawartość bez monitorowania, kliknij opcję **W<sup>31</sup>cz**. Wszystkie uprawnienia w polu **Dodatkowe niepodpisane uprawnienia** mają przypisaną wartość **W<sup>31</sup>cz**; nie można indywidualnie zresetować żadnego uprawnienia do wartości **Wy<sup>31</sup>cz**.

### Uruchamiaj podpisane zawartość

Uprawnienia możesz określić indywidualnie, ustawiając w polu **Uruchamiaj podpisane zawartość** wartość **Monituj**, która ustawia wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** na wartość **Monituj**. Następnie możesz zresetować oddzielnie każde uprawnienie, nadając mu wartość **Wy<sup>31</sup>cz** lub **W<sup>31</sup>cz**. Jeżeli wybierzesz wartość **Wy<sup>31</sup>cz** lub **W<sup>31</sup>cz**, ustawienie to będzie stosowane dla wszystkich uprawnień w obszarze **Dodatkowe podpisane uprawnienia**.

Wybierz jedną z następujących możliwości dla pola **Uruchamiaj podpisane zawartość**:

- Aby uzyskiwać monity o akceptację przed uruchomieniem apletu Java z jego wymaganymi uprawnieniami, kliknij opcję **Monituj**. Jeżeli wybierzesz opcję **Monituj** w polu **Uruchamiaj podpisane zawartość**, wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** mają przypisaną wartość **Monituj** i można każde z nich indywidualnie zresetować do wartości **Wy<sup>31</sup>cz** lub **W<sup>31</sup>cz**.
- Aby automatycznie odrzucać uruchamianie podpisanej zawartości bez monitorowania, kliknij opcję **Wy<sup>31</sup>cz**. Wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** mają przypisaną wartość **Wy<sup>31</sup>cz**; nie można indywidualnie zresetować żadnego uprawnienia do wartości **Monituj** lub **W<sup>31</sup>cz**.
- Aby automatycznie akceptować uruchamianie nie podpisanej zawartości bez monitorowania, kliknij opcję **W<sup>31</sup>cz**. Wszystkie uprawnienia w polu **Dodatkowe podpisane uprawnienia** mają przypisaną wartość **W<sup>31</sup>cz**; nie można indywidualnie zresetować żadnego uprawnienia do wartości **Monituj** lub **Wy<sup>31</sup>cz**.

Zamyka to okno dialogowe i zapisuje wprowadzone zmiany.

Kliknij, aby zresetować wszystkie uprawnienia Java. Wybierz jedną z następujących opcji, a następnie kliknij przycisk **Resetuj**.

- **Zapisane uprawnienia** Resetuje do ostatnich zapisanych uprawnień. Wszystkie zmiany wprowadzone od czasu ostatniego zapisu ustawień zostaną utracone.
- **Wysoki poziom zabezpieczeń** Resetuje do uprawnień wysokiego bezpieczeństwa (najbardziej restrykcyjne, applety działają w trybie bezpiecznym). Wszystkie uprawnienia w polu **Uruchamiaj podpisane zawartości** resetowane do wartości **Monituj**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartości **Wyłącz**.
- **Średni poziom zabezpieczeń** Resetuje do uprawnień średniego bezpieczeństwa (applety działają w piaskownicy z dwoma dodatkowymi restrykcjami, Przestrzeń dostępna i Dostęp do plików wybrany przez użytkownika). Wszystkie uprawnienia (oprócz Przestrzeń dostępna i Dostęp do plików wybrany przez użytkownika) w polu **Uruchamiaj podpisane zawartości** resetowane do wartości **Monituj**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartości **Wyłącz**.
- **Niski poziom zabezpieczeń** Resetuje do uprawnień niskiego bezpieczeństwa (najmniej restrykcyjne, applety działają ze wszystkimi uprawnieniami). Wszystkie uprawnienia w polu **Uruchamiaj podpisane zawartości** resetowane do wartości **Wyłącz**, a w polu **Dodatkowe niepodpisane uprawnienia** do wartości **Wyłącz**.

## Przeглядanie uprawnień - karta

Te uprawnienia Java okreœlonymi przez administratora sieci.

Aby aplet Java mógł dzia³aæ, mo¿e wymagaæ dostêpu do plików i innych zasobów komputera. Czynnoœci te wymagaj¹ specjalnych uprawnieñ, które musz¹ byæ udzielone przed ich podjêciem. Administrator sieci mógł ju¿ okreœliæ, jakie uprawnienia s¹ dozwolone. Dla dozwolonych uprawnieñ administrator sieci mo¿e okreœliæ, czy bêd¹ pojawia³y siê powiadomienia o wymaganiu tych uprawnieñ. W przeciwnym przypadku powiadomienia pojawiaj¹ siê jedynie wówczas, gdy aplet Java wymaga wiêcej uprawnieñ ni¿ zosta³o to automatycznie przydzielone przez administratora sieci.

Istniej¹ nastêpuj¹ce trzy zestawy uprawnieñ:

**Uprawnienia nadane niepodpisanej zawartoœci** Uprawnienia przydzielone pobranej zawartoœci nie podpisanej (aplety bêd¹ uruchamiane w piaskownicy).

**Uprawnienia, które podpisana zawartoœæ posiada** Uprawnienia, które nie wymagaj¹ potwierdzenia przez u¿ytkownika.

**Uprawnienia, które podpisanej zawartoœci zosta³y odmówione** Uprawnienia, które wymagaj¹ potwierdzenia przez u¿ytkownika lub s¹ absolutnie zakazane.

Mo¿esz klikn¹æ dwukrotnie nag³ówek ka¿dego z uprawnieñ, aby wyœwietliæ konkretne uprawnienia i okreœlone ustawienia.

Zestawom tym mo¿na przypisaæ nastêpuj¹ce uprawnienia:

[Dostêp do interfejsu u¿ytkownika](#)

[Drukowanie](#)

[Informacje o systemie](#)

[Magazyn klienta](#)

[Multimedia](#)

[Niestandardowe](#)

[Operacje I/O na plikach](#)

[Operacje I/O sieci](#)

[Operacje I/O u¿ytkownika na plikach](#)

[Refleksja](#)

[Rejestr](#)

[W³tki](#)

[W³aœciwoœæ](#)

[Wykonanie](#)

[Zabezpieczenie](#)

Uprawnienie, które kontroluje dostęp do odczytu, zapisu i usuwania plików.

Uprawnienie, które kontroluje możliwość wykonywania operacji sieciowych lub czynności związanych z siecią.

Uprawnienie, które kontroluje możliwość tworzenia w³tków i grup w³tków oraz manipulowania nimi.

Uprawnienie, które kontroluje możliwość dostępu do globalnych w³aœciwoœci systemu i manipulowania nimi.



Uprawnienie, które kontroluje możliwość uruchamiania innych programów.

Uprawnienie, które kontroluje możliwość użycia interfejsu Reflection API w celu uzyskania dostępu do elementów podanej klasy.

Uprawnienie, które kontroluje dostęp do interfejsów API drukowania.

Uprawnienie, które kontroluje możliwość uzyskania dostępu do rejestru.

Uprawnienie, które kontroluje dostęp dla klas zabezpieczeń JDK, `java.lang.security`.

Uprawnienie do kontrolowania dostępu do magazynu po stronie klienta, który jest dostępny przez klasę ClientStore.

Uprawnienie, które kontroluje możliwość użycia niektórych rozszerzonych funkcji AWT.

Uprawnienie, które kontroluje dostęp do informacji systemowych.



Uprawnienie, które kontroluje możliwość wyświetlania okien dialogowych plików do operacji na plikach. Na przykład, jeśli aplet wymaga otwarcia pliku, musi skorzystać ze standardowego okna dialogowego **Otwórz plik**, aby następnie pozwolić wybrać użytkownikowi plik do otwarcia. Aplet nie będzie mógł wykonywać operacji na plikach samodzielnie. Dzięki temu operacja jest bezpieczniejsza niż w przypadku kodu realizującego bezpośredni dostęp do pliku, ponieważ wymaga bezpośredniego zaangażowania użytkownika. Poziom tego uprawnienia jest określany jako średni.

Uprawnienie, które kontroluje użycie rozszerzonych funkcji multimedialnych.

Uprawnienie, które zapewnia możliwość dokładnej kontroli rodzaju uprawnień udzielanych podpisanej zawartości.

Uprawnienie, które kontroluje możliwość tworzenia do 1 MB miejsca pomocniczego przez kod podpisany, które może być wykorzystywane do przechowywania tymczasowych informacji. Aplet Java nie będzie mógł czytać ani zapisywać żadnych innych plików na dysku twardym użytkownika. Podpisany aplet może mieć dostęp jedynie do własnego miejsca pomocniczego. Poziom tego uprawnienia jest określany jako średni.

Uprawnienie, które kontroluje możliwość przedstawiania okien dialogowych.

Środowisko chroni ści pewne zasoby (na przyk³ad system, dysk twardy, sieæ, komputer lokalny itd.) przed dostêpem z zewn¹trz, w którym aplet Java mo¿e byæ uruchomiony z kontrolowanym przez u¿ytkownika zestawem uprawnieñ.

